# CLAIM AMENDMENTS

## Claim Amendment Summary

**Claims pending**

- Before this Amendment: Claims 1-20 and 26-38.
- After this Amendment: Claims 1-20 and 26-38.

**Non-Elected, Canceled, or Withdrawn claims**: 21-25 and 39-43.

**Amended claims**: 1, 7-12, 20, 26, and 36-38.

**New claims**: none.

---

## Claims:

**1.** **(Currently Amended)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method for protecting digital media comprising:

obtaining a message $M$ having two portions, wherein $M_1$ is one of the portions of the $M$ and $M_2$ is another;

generating one or more codes having a combination with $M_2$ implicitly embedded therein, wherein calculations that generate the one or more codes do not employ $M_2$ and $M_2$ cannot be derived from these calculations of one or more codes;

reporting the one or more codes, by which reporting the one or more codes facilitates a cryptographic technique for protecting digital media.

**2.** **(Original)** A medium as recited in claim 1, wherein the method further comprises producing a digital signature (*DS*) comprising $M_1$ and the reported one or more codes.

**3.** **(Original)** A medium as recited in claim 1, wherein two or more codes are generated by the generating and reported by the reporting.

**4.** **(Original)** A medium as recited in claim 3, wherein a mathematical function for calculating one code is not identical to a mathematical function for calculating another code.

**5.** **(Original)** A medium as recited in claim 3, wherein the message *M* has a defined length and a length of a combination of two or more codes is less than the message's defined length.

**6.** **(Original)** A medium as recited in claim 3, wherein $M_2$ has a defined length and a length of a combination of two or more codes is less than or equal to the defined length of $M_2$.

**7.** **(Currently Amended)** A medium as recited in claim 1, wherein the generating comprises:

finding a value of a variable per-message key (*k*) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing *k* produces a result equivalent to $M_2$, wherein g is a fixed element of order q in a fixed group, and $H_0$ is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of $k$ is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates $k$.

**8. (Currently Amended)** A medium as recited in claim 1, wherein the generating comprises:

finding a value of a variable per-message key ($k$) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing $k$ produces a result equivalent to $M_2$, wherein g is a fixed element of order q in a fixed group, and $H_0$ is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of $k$ is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code, the calculation of at least one code employs non-linear mathematical function, ~~namely a quadratic equation,~~ and where each calculation incorporates $k$.

**9. (Currently Amended)** A medium as recited in claim 3, wherein the generating comprises:

finding a value of a variable per-message key ($k$) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing $M_1$ and $g^k$ produces a result equivalent to $M_2$, wherein g is a fixed element of order q in a fixed group, and $H_0$ is a predefined hash function instantiated by using a keyed version of a secure hash function;

when such a value of $k$ is found, calculating the two or more codes, where one code is $r$ and another is $s$, with $r$ being calculated using another predefined mathematical function employing $M_1$ and $g^k$, and with $s$ being calculated using still another predefined mathematical function employing $M_1$ and $g^k$ and $r$.

**10.** **(Currently Amended)** A medium as recited in claim 3, wherein the method further comprises producing a digital signature (*DS*) comprising $M_1$ and the reported codes~~ r and s~~.

**11.** **(Currently Amended)** A computing device comprising:

an ~~audio/visual~~ output peripheral device;

a medium as recited in claim 1.

**12.** **(Currently Amended)** A computer-readable medium having computer-executable instructions that, when executed by a computer, performs a method comprising:

obtaining a message $M$ having two portions, wherein $M_1$ is one of the portions of the $M$ and $M_2$ is another;

generating two or more codes having a combination with $M_2$ implicitly embedded therein, wherein calculations that generate the codes do not employ $M_2$ and $M_2$ cannot be derived from these calculations of one or more codes, wherein the generating comprises:

- finding a value of a variable per-message key ($k$) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing $M_1$ and $g^k$ produces a result equivalent to $M_2$, wherein g is a fixed element of order q in a fixed group, and $H_0$ is a predefined hash function instantiated by using keyed versions of a secure hash function;

- when such a value of $k$ is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates $k$;

reporting the two or more codes, by which reporting the two or more codes facilitates a cryptographic technique for protecting digital media.

**13.** **(Original)** A medium as recited in claim 12, wherein the method further comprises producing a digital signature (*DS*) comprising $M_1$ and the reported two or more codes.

**14.** **(Original)** A medium as recited in claim 12, wherein the calculation of at least one code employs a non-linear mathematical function.

**15.** **(Original)** A medium as recited in claim 12, wherein the message $M$ has a defined length and a length of a combination of two or more codes is less than the message's defined length.

**16.** **(Original)** A medium as recited in claim 12, wherein $M_2$ has a defined length and a length of a combination of two or more codes is less than or equal to the defined length of $M_2$.

**17.** **(Original)** A medium as recited in claim 12, wherein one calculated code is $r$ and another is $s$, with $r$ being calculated using another predefined mathematical function employing $M_1$ and $g^k$, and with $s$ being calculated using still another predefined mathematical function employing $M_1$ and $g^k$ and $r$.

**18.** **(Original)** A medium as recited in claim 17, wherein the predefined mathematical function for $s$ is non-linear.

**19.** **(Original)** A medium as recited in claim 17, wherein the method further comprises producing a digital signature ($DS$) comprising $M_1$ and the reported codes $r$ and $s$.

**20.** **(Currently Amended)** A computing device comprising:

an ~~audio/visual~~ output peripheral device;

a medium as recited in claim 12.

**Claims 21-25 are CANCELED.**

**26.** **(Original)** A method for facilitating digital security, the method comprising:

obtaining a message $M$ having two portions, wherein $M_1$ is one of the portions of the $M$ and $M_2$ is another;

generating two or more codes having a combination with $M_2$ implicitly embedded therein, wherein calculations that generate the codes do not employ $M_2$ and $M_2$ cannot be derived from these calculations of one or more codes, wherein the generating comprises:

- finding a value of a variable per-message key ($k$) where a predefined mathematical function, $M_2 = H_0(M_1, g^k)$, employing $M_1$ and $g^k$ produces a result equivalent to $M_2$, wherein g is a fixed element of order q in a fixed group, and $H_0$ is a predefined hash function instantiated by using keyed versions of a secure hash function;
- when such a value of $k$ is found, calculating the two or more codes, where the calculation of one code is not identical to the calculation of any other code and where each calculation incorporates $k$;

reporting the two or more codes, by which reporting the two or more codes facilitates a cryptographic technique for protecting digital media.

**27.** **(Original)** A method as recited in claim 1 further comprising producing a digital signature ($DS$) comprising $M_1$ and the reported two or more codes.

**28.** **(Original)** A digital signature ($DS$) produced by a method as recited in claim 27 and embodied on a computer-readable medium.

**29.** **(Original)** A digital signature (*DS*) produced by a method as recited in claim 27 and embodied as human-readable indicia on a human-readable medium.

**30.** **(Original)** A method as recited in claim 1, wherein the calculation of at least one code employs a non-linear mathematical function.

**31.** **(Original)** A method as recited in claim 1, wherein the message $M$ has a defined length and a length of a combination of two or more codes is less than the message's defined length.

**32.** **(Original)** A method as recited in claim 1, wherein $M_2$ has a defined length and a length of a combination of two or more codes is less than or equal to the defined length of $M_2$.

**33.** **(Original)** A method as recited in claim 1, wherein one calculated code is $r$ and another is $s$, with $r$ being calculated using another predefined mathematical function employing $M_1$ and $g^k$, and with $s$ being calculated using still another predefined mathematical function employing $M_1$ and $g^k$ and $r$.

**34.** **(Original)** A method as recited in claim 33, wherein the predefined mathematical function for $s$ is non-linear.

**35.** **(Original)** A method as recited in claim 33, wherein the predefined mathematical function for *s* is quadratic.

**36.** **(Currently Amended)** A method as recited in claim 1 further comprising producing a message comprising $M_1$ and the reported codes ~~*r* and *s*~~.

**37.** **(Currently Amended)** A computer-readable medium embodying a message produced by a method as recited in claim 36, by which the message functions with a processor to protect digital media ~~and embodied on a computer-readable medium~~.

**38.** **(Currently Amended)** A method comprising:

producing a message produced by a method as recited in claim 36 ~~and embodied~~ as human-readable indicia on a human-readable medium.

**Claims 39-43 are CANCELED.**